AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

ANTHONY MANCILLA-MARQUEZ,
aka "Fox,"

Defendant

Case No. 2:24-mj-05590-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of June 12, 2024, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Possession with Intent to Distribute a Controlled Substance (Fentanyl)

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Brandon Purece, Task Force Officer
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: September 16, 2024

Judge's signature

City and state: Los Angeles, California

Hon. Stephanie Christensen, U.S. Magistrate Judge
Printed name and title

AUSA: Kelsey Stimson x8230

AFFIDAVIT

I, Brandon C. Purece, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrant against ANTHONY MANCILLA-MARQUEZ ("MANCILLA"), also known as "Fox," for a violation of 21 U.S.C. § 841(a)(1): Possession with Intent to Distribute Controlled Substances.

2. This affidavit is also made in support of an application for a warrant to search the following digital device in the custody of the Los Angeles Police Department, in Los Angeles, California, as described more fully in Attachment A: a black Motorola cellphone with a cracked screen, inside a blue rubber case with a SIM card, logged with the Los Angeles Police Department as Property Item No. 9 under the case number identified in Attachment A (the "SUBJECT DEVICE").

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances) and 18 U.S.C. §§ 922(g) (prohibited person in possession of a firearm) and 924(c) (possession of a firearm in furtherance of a drug trafficking crime) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and part only.

II. BACKGROUND OF AFFIANT

5. I am a Task Force Officer ("TFO") with United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), currently assigned to the Los Angeles Field Division, Group II / Los Angeles Police Department ("LAPD"), Metropolitan Division Task Force. I have been a peace officer for the LAPD for over 28 years. My mission within this task force includes reducing gang-related and violent crime, assisting in the investigation, identification, location, and apprehension of persons that have committed crimes within the City of Los Angeles or against the United States, and utilizing proactive methods to monitor and prevent criminal activity. I have been assigned to the Metropolitan Division / ATF Task Force for approximately three years.

6. I received seven months of basic law enforcement training while attending the Los Angeles Police Academy. I have also received several specialized training blocks in narcotics

and firearms and received additional training from more experience police officers and federal agents. I have been assigned to uniformed gang assignments with the Los Angeles Police Department in 77th, Foothill, Southwest, Rampart, and Hollywood Divisions. I spent an additional three years as a Task Force Officer with the Federal Bureau of Investigation involved in investigating criminal activity of street gangs in the City of Los Angeles. During my time as a peace officer and a task force officer, I have conducted hundreds of firearms and narcotic related investigations, including conducting surveillance at known narcotics, gang, and illegal firearm sales locations and observing the actions and methods utilized by offenders in the course of buying and selling contraband. I have arrested numerous persons for illegally possessing firearms and narcotics.

III. SUMMARY OF PROBABLE CAUSE

7. On September 18, 2023, Los Angeles Police Department ("LAPD") officers drove past MANCILLA and saw that he had a satchel slung across his chest. The officers drove back to MANCILLA to make contact and saw he no longer had the satchel. The officers searched the area and found the satchel. They recovered a loaded .380 caliber, semi-automatic pistol inside.

8. On June 12, 2024, LAPD officers saw MANCILLA driving a car with expired registration. The officers attempted a traffic stop, but MANCILLA fled. The officers later caught MANCILLA running away from his car and took him into custody. Officers recovered from MANCILLA's car what drug testing later confirmed

to be a mixture or substance containing a detectable amount of methamphetamine and fentanyl, along with other indicia of drug trafficking, and a loaded 9mm, privately manufactured, semi-automatic pistol.

IV. STATEMENT OF PROBABLE CAUSE

9. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

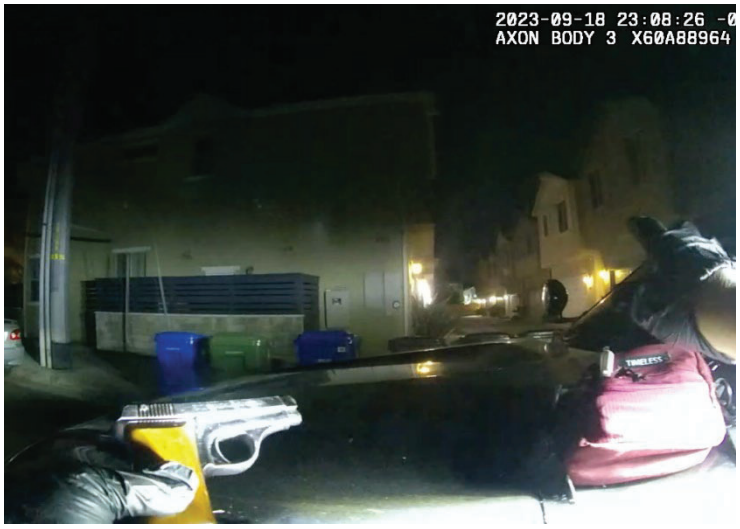
A. September 18, 2023: LAPD Officers Recover a Loaded Firearm During a Pedestrian stop of MANCILLA.

10. According to law enforcement reports, on September 18, 2023, at approximately 11:10 p.m., LAPD patrol officers Edgar Amaya and Mark Gonzales were driving east on Kittridge Street from Vineland Avenue when they saw MANCILLA walking on the sidewalk in the opposite direction. The officers saw MANCILLA was wearing a satchel across his chest when they passed him. The officers were aware that the area was claimed by North Hollywood Boyz criminal street gang and that MANCILLA was wearing a Boston Red Sox Major League Baseball cap, which the officers were aware is commonly worn by North Hollywood Boyz gang members to indicate gang affiliation.

11. The officers conducted a U-turn and pulled up adjacent to MANCILLA, who was no longer wearing the satchel. MANCILLA told the officers that he was on probation. The officers ran MANCILLA and learned that he was on Post Release Community Supervision ("PRCS"). The officers were aware that PRCS has

standard search and seizure conditions, so they conducted a compliance search.

12. With his body worn camera on, Officer Amaya walked the path that MANCILLA had been walking and could not find the satchel. Both officers then searched for the satchel and Officer Amaya recovered a red satchel from the street in the area where they had seen MANCILLA walking. Inside the satchel, the officers found a Tanfoglio GT380 model, .380 caliber, semi-automatic pistol loaded with three live .380 caliber rounds.



13. Also in the satchel, the officers found a scale with white powder residue, suspected to be methamphetamine, and an empty syringe.

14. The pistol, magazine of the pistol, and satchel were all swabbed for DNA and compared to a sample of MANCILLA's DNA. The DNA results were inconclusive.

15. In a post-Miranda interview on the scene of the arrest, MANCILLA told the officers that the red satchel was not his but that he had a satchel and he "threw [his] shit somewhere

else." MANCILLA directed the officers towards down the street and said, "I threw it in the front yard . . . right there." The officers canvassed the area where MANCILLA had indicated he had thrown his item but did not find another satchel.

B. June 12, 2024: LAPD Officers Recover a Loaded Firearm and Drug-Trafficking Indicia from MANCILLA.

16. According to law enforcement reports, on June 12, 2024, at approximately 10:56 p.m., LAPD North Hollywood Division patrol officers Fernando Olmos and Alejandro Flores were driving west on Sherman Way from Vineland when they saw a 2003 Lexus ES300, California license plate 5CLZ202, driving the opposite direction on Sherman Way. As they passed the Lexus, the officers recognized MANCILLA as the driver and only occupant of the car based on photographs and information they previously received from gang officers at North Hollywood Division. The officers were aware that MANCILLA was an active North Hollywood Boyz gang member and saw that MANCILLA was wearing a Boston Red Sox Major League Baseball cap, which is consistent with affiliation with the North Hollywood Boyz criminal street gang. The officers ran the license plate to the Lexus and found that the registration was expired.[1]

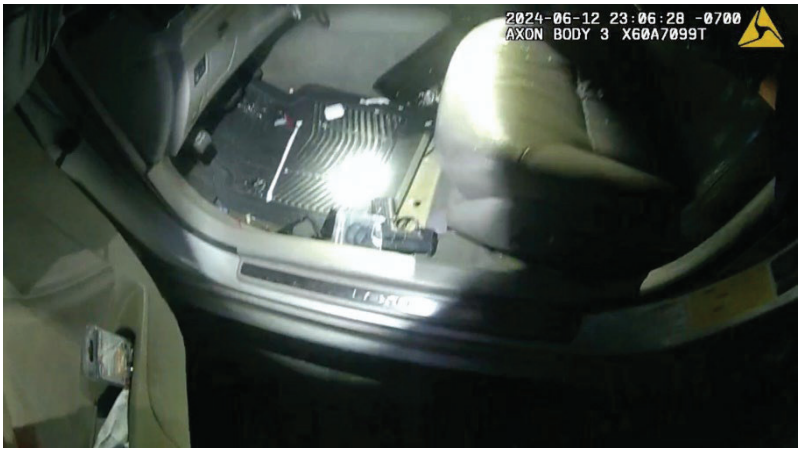
17. The officers then attempted to conduct a traffic stop on MANCILLA for a violation of California Vehicle Code § 4000(a) (Expired Registration). The officers conducted a U-turn, pulled up adjacent to MANCILLA's vehicle, and activated the police

[1] The license plate indicated that the car was registered to E.K. in Manhattan Beach, California.

car's emergency equipment three separate times, but MANCILLA failed to yield. Instead, MANCILLA conducted a U-turn and accelerated, fleeing from the officers.

18. The officers were aware that MANCILLA had previously frequented a recreational vehicle encampment near Fair Avenue and Sherman Way. The officers drove directly to that area after MANCILLA fled. When the officers arrived, they saw MANCILLA running away from the Lexus, which had been parked along the curb of Fair Avenue. MANCILLA appeared to see the officers, turn, and run away. The officers pursued MANCILLA on foot, eventually catching up to MANCILLA and taking him into custody.

19. Meanwhile, additional officers went to MANCILLA's vehicle and looked inside the windows. They saw, in plain view, a pistol on the driver's floorboard. The officers recovered the pistol and learned that it was an un-serialized, privately manufactured, 9mm, semi-automatic pistol loaded with six live 9mm rounds, including one live round in the chamber.[2]



[2] The officers took a DNA swab of the pistol and magazine and a comparison request is pending against MANCILLA's DNA.

20. The officers also found and seized from the car a Boston Red Sox cap, a Motorola cellphone, as well as indicia of drug-trafficking, namely: two scales, $492 in various denominations, a pay-owe notebook, plastic baggies, and approximately 215 grams of suspected methamphetamine and suspected cocaine that had been strewn about the car's interior.

21. In a post-Miranda interview, MANCILLA confirmed that the Lexus was his but denied that he had been driving it. He also confirmed that the cellphone found inside the car was his.

22. On June 14, 2024, laboratory results from the LAPD Forensic Science Division determined that the suspected narcotics recovered from MANCILLA's car were approximately 184.72 grams of a mixture and substance containing a detectable amount of methamphetamine and 14.23 grams of a mixture and substance containing a detectable amount of fentanyl.

C. MANCILLA Has Multiple Prior Felony Convictions.

23. On or around July 29, 2024, I reviewed MANCILLA's criminal history using the California Law Enforcement Telecommunications System ("CLETS") and National Crime Information Center ("NCIC") databases. Based on my review of this information, I learned that MANCILLA has previously been convicted of the following felony crimes, each punishable by a term of imprisonment exceeding one year:

a. On or about July 8, 2016, MANCILLA was convicted of Possession of a Firearm by a Felon, in violation of California Penal Code Section 29800(a)(1), in the Superior Court

of the State of California, County of Los Angeles, in case number LA083396;

b. On or about July 8, 2016, MANCILLA was convicted of Prohibited Ownership of Ammunition, in violation of California Penal Code Section 30305(a)(1), in the Superior Court of the State of California, County of Los Angeles, in case number LA083396;

c. On or about August 23, 2016, MANCILLA was convicted of Driving a Vehicle Without Owner's Consent, in violation of California Vehicle Code Section 18051(a), in the Superior Court of the State of California, County of Los Angeles, in case number LA083922;

d. On or about August 23, 2016, MANCILLA was convicted of a Hit and Run, in violation of California Vehicle Code Section 20001(b)(1), in the Superior Court of the State of California, County of Los Angeles, in case number LA083922;

e. On or about December 14, 2017, MANCILLA was convicted of Robbery, in violation of California Penal Code Section 211, in the Superior Court of the State of California, County of Los Angeles, in case number PA089843;

f. On or about January 23, 2018, MANCILLA was convicted of Fleeing a Pursuing Officer Vehicle while Driving Recklessly, in violation of California Vehicle Code Section 2800.2 in the Superior Court of the State of California, County of Los Angeles, in case number LA087252;

g. On or about February 14, 2022, MANCILLA was convicted of Possession of a Firearm by a Felon, in violation of

California Penal Code Section 29800(a)(1), in the Superior Court of the State of California, County of Los Angeles, in case number LA096086.

24. Based on my review of MANCILLA's criminal history and the arrest reports for the above referenced LAPD arrests, MANCILLA was on active PRCS at the time he allegedly possessed a firearm on September 18, 2023, and on June 12, 2024.

D. Interstate Nexus

16. On August 29, 2024, an ATF Interstate Nexus Expert examined the firearms and ammunition recovered during each of MANCILLA's arrests described above. The expert determined:

a. The firearm recovered on September 18, 2023 -- an Armi Tanfoglio, model GT 380, .380 ACP caliber semi-automatic pistol, bearing serial number T71148 -- was manufactured in Italy;

b. The ammunition recovered on September 18, 2023 -- three live rounds of Winchester, .380 Auto caliber ammunition, marked with the headstamp "WIN 380 AUTO" -- were manufactured in Illinois or Mississippi;

c. Five rounds of the ammunition recovered on June 12, 2024 -- five rounds of Cascade Cardrige Inc. (CCI), 9mm Luger caliber ammunition, marked with the headstamp "CCI NR 9mm Luger" -- were manufactured in Idaho; and

d. One round of ammunition recovered on June 12, 2024 -- one round of Arms Corporation of the Philippines

(Armscor), 9mm Luger caliber ammunition, marked with the headstamp "A USA 9mm Luger" -- was manufactured in the Philippines.

17. The un-serialized firearm recovered on June 12, 2024, was not tested because it is a privately manufactured firearm (i.e., a "ghost gun") and therefore interstate or foreign transportation of the firearm cannot be determined.

18. Because the firearm and ammunition recovered on September 18, 2023, and the ammunition recovered on June 12, 2024, was not manufactured in California, they must have traveled in interstate or foreign commerce before coming into MANCILLA's possession, and therefore they affected interstate and/or foreign commerce.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

19. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to

diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

VI. TRAINING AND EXPERIENCE ON FIREARMS OFFENSES

20. From my training, personal experience, and the collective experiences related to me by other law enforcement officers who conduct who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such in their digital devices. It has been my experience that prohibited individuals who own firearms illegally will keep the contact information of the individual who is supplying firearms to prohibited individuals or other individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

c. Those who illegally possess firearms often sell their firearms and purchase firearms. Correspondence between persons buying and selling firearms often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience, individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with each other regarding firearms that the sell or offer for sale. In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

d. Individuals engaged in the illegal purchase or sale of firearms and other contraband often use multiple digital devices.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[3]

21. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

[3] As used herein, the term "digital device" includes the SUBJECT DEVICE and any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral

(footnote cont'd on next page)

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the

---

input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

22. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so

many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

a. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

23. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. CONCLUSION

24. For all of the reasons described above, there is probable cause to believe that on or about June 12, 2024, MANCILLA committed a violation of 21 U.S.C. § 841(a)(1): Possession with Intent to Distribute Controlled Substances. There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICE described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 16th day of September, 2024.

HONORABLE STEPHANIE S. CHRISTENSEN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following digital device (the "SUBJECT DEVICE"), seized on June 12, 2024, and currently maintained in the custody of the Los Angeles Police Department in Los Angeles, California: black Motorola cellphone with a cracked screen, inside a blue rubber case with a SIM card, logged with the Los Angeles Police Department as Property Item No. 9 under case number 24-1511255.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) (possession with intent to distribute controlled substances) and 846 (conspiracy and attempt to distribute controlled substances) and 18 U.S.C. §§ 922(g) (prohibited person in possession of a firearm) and 924(c) (possession of a firearm in furtherance of a drug trafficking crime) (the "Subject Offenses"), namely:

a. Records, documents, programs, applications and materials, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

c. Records, documents, programs, applications or materials, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

d. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs, firearms, or ammunition;

e. Contents of any calendar or date book which related to the above-named violations or occurring after January 1, 2023;

f. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; which related to the above-named violations or occurring after January 1, 2023; and

g. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

h. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

4. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The

government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be

seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the

custody and control of attorneys for the government and their support staff for their independent review.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.